Publicatieblad
van de Europese Unie

NL
L-serie

2025/908

23.5.2025

BESLUIT Nr. 1/2024 VAN HET GEMENGD COMITÉ DAT IS OPGERICHT BIJ DE OVEREENKOMST TUSSEN DE EUROPESE UNIE EN DE ZWITSERSE BONDSSTAAT INZAKE DE KOPPELING VAN HUN REGELINGEN VOOR DE HANDEL IN BROEIKASGASEMISSIERECHTEN

van 4 december 2024

wat betreft de wijziging van bijlage II bij de overeenkomst en van de gemeenschappelijke operationele procedures en de koppelingstechnische normen [2025/908]

HET GEMENGD COMITÉ,

Gezien de Overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten ([1]) ("de overeenkomst"), en met name artikel 9 en artikel 13, lid 2,

Overwegende hetgeen volgt:

(1) Besluit nr. 2/2019 van het Gemengd Comité ([2]) voorzag in een voorlopige oplossing om de koppeling tussen het EU-ETS en het ETS van Zwitserland te realiseren.

(2) Tijdens zijn derde vergadering heeft het Gemengd Comité overeenstemming bereikt over de noodzaak om de kosteneffectiviteit van een permanente koppeling tussen het register van de Unie en het Zwitserse register te analyseren.

(3) Tijdens zijn vijfde vergadering heeft het Gemengd Comité overeenstemming bereikt over het verslag van de bij Besluit nr. 1/2020 ([3]) en Besluit nr. 2/2020 ([4]) van het Gemengd Comité opgerichte werkgroep. In dat verslag heeft de werkgroep een aanpak voor de uitvoering van de permanente koppeling tussen het register van de Unie en het Zwitserse register geanalyseerd en aanbevolen.

(4) Om rekening te houden met de technische vereisten van de permanente koppeling tussen het register van de Unie en het Zwitserse register, en om de bepalingen van bijlage II bij de overeenkomst te stroomlijnen in het licht van de technologische ontwikkelingen, moet bijlage II bij de overeenkomst worden gewijzigd.

(5) Om te zorgen voor consistentie van de gemeenschappelijke operationele procedures en de koppelingstechnische normen met bijlage II bij de overeenkomst, moeten die documenten ook worden aangepast,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

1. Bijlage II bij de overeenkomst wordt vervangen door de tekst in bijlage I bij dit besluit.

2. De in artikel 3, lid 6, van de overeenkomst bedoelde gemeenschappelijke operationele procedures zijn opgenomen in bijlage II bij dit besluit. Zij vervangen de gemeenschappelijke operationele procedures in de bijlage bij Besluit nr. 1/2020.

([1]) PB L 322 van 7.12.2017, blz. 3.
([2]) Besluit nr. 2/2019 van het Gemengd Comité dat is opgericht bij de Overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten van 5 december 2019 tot wijziging van de bijlagen I en II bij de Overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten [2020/1359] (PB L 314 van 29.9.2020, blz. 68).
([3]) Besluit nr. 1/2020 van het Gemengd Comité dat is opgericht bij de Overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten van 5 november 2020 betreffende de vaststelling van gemeenschappelijke operationele procedures [2021/1033] (PB L 226 van 25.6.2021, blz. 2).
([4]) Besluit nr. 2/2020 van het Gemengd Comité dat is opgericht bij de Overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten van 5 november 2020 met betrekking tot de wijziging van de bijlagen I en II bij de overeenkomst en tot vaststelling van koppelingstechnische normen (LTS) [2021/1034] (PB L 226 van 25.6.2021, blz. 16).

3. De in artikel 3, lid 7, van de overeenkomst bedoelde koppelingstechnische normen zijn opgenomen in bijlage III bij dit besluit. Zij vervangen de koppelingstechnische normen in de bijlage bij Besluit nr. 2/2020.

Artikel 2

Dit besluit treedt in werking op de dag van de vaststelling ervan.

Gedaan te Brussel, 4 december 2024.

Voor het Gemengd Comité

Secretaris voor de Europese Unie	*De voorzitter*	*Secretaris voor Zwitserland*
Ruben VERMEEREN	Beatriz YORDI	Thomas MEIER

BIJLAGE I

"BIJLAGE II

KOPPELINGSTECHNISCHE NORMEN

Om de koppeling tussen het EU-ETS en de ETS van Zwitserland operationeel te maken, is in 2020 een voorlopige oplossing ingevoerd. Met ingang van 2023 zal de registerkoppeling tussen de twee emissiehandelsregelingen zich geleidelijk ontwikkelen tot een permanente registerkoppeling die naar verwachting uiterlijk in 2024 tot stand zal worden gebracht en die de werking van de gekoppelde markten met betrekking tot de voordelen van marktliquiditeit en de uitvoering van transacties tussen de twee gekoppelde systemen mogelijk maakt op een wijze die gelijkwaardig is aan één markt die uit twee systemen bestaat en die marktdeelnemers in staat stelt op te treden alsof zij zich op één markt bevonden, behoudens individuele regelgeving van de partijen.

In de koppelingstechnische normen (LTS) moet het volgende worden aangegeven:

— de architectuur van de communicatieverbinding;

— de communicatie tussen het SSTL en het EUTL;

— de beveiliging van de gegevensoverdracht;

— de lijst van functies (transacties, verzoening enz.);

— de definitie van de transportlaag;

— de vereisten inzake gegevensopslag;

— het operationele plan (call desk, ondersteuning);

— het communicatieactiveringsplan en de testprocedure;

— de procedure om de beveiliging te testen.

In de LTS moet worden vermeld dat de administrateurs redelijke stappen moeten ondernemen om ervoor te zorgen dat het SSTL, het EUTL en de koppeling 24 uur per dag en zeven dagen per week operationeel zijn en dat onderbrekingen in de activiteiten van het SSTL, het EUTL en de koppeling zo veel mogelijk worden beperkt.

De LTS moeten extra beveiligingsvoorschriften bevatten voor het Zwitserse register, het SSTL, het register van de Unie en het EUTL en moeten in een "veiligheidsbeheersplan" worden gedocumenteerd. In de LTS moet met name worden vermeld dat:

— indien het vermoeden bestaat dat de veiligheid van het Zwitserse register, het SSTL, het register van de Unie of het EUTL in het gedrang is gekomen, beide partijen elkaar daarvan onverwijld in kennis moeten stellen en de koppeling tussen het SSTL en het EUTL moeten onderbreken;

— in geval van een beveiligingsinbreuk verbinden de partijen zich ertoe de informatie onmiddellijk met elkaar te delen. Indien de technische details beschikbaar zijn, moet binnen 24 uur nadat een beveiligingsincident als een beveiligingsinbreuk is aangemerkt, een rapport met een beschrijving van het incident (datum, oorzaak, effect, genomen maatregelen) tussen de Zwitserse registeradministrateur en de centrale administrateur van de Unie worden uitgewisseld.

De in de LTS beschreven procedure om de beveiliging te testen, moet worden voltooid voordat de communicatieverbinding tussen het SSTL en het EUTL tot stand wordt gebracht en wanneer een nieuwe versie of release van het SSTL of het EUTL is vereist.

De LTS moeten, naast de productieomgeving, in twee testomgevingen voorzien: een ontwikkelingstestomgeving en een acceptatieomgeving.

De partijen moeten via de Zwitserse registeradministrateur en de centrale administrateur van de Unie het bewijs leveren dat er in de voorafgaande twaalf maanden een onafhankelijke beoordeling van de veiligheid van hun systemen volgens de veiligheidsvoorschriften van de LTS is uitgevoerd. Op alle nieuwe belangrijke releases van de software moeten veiligheidstests en vooral penetratietests worden uitgevoerd volgens de veiligheidsvoorschriften van de LTS. De penetratietests mogen niet door de softwareontwikkelaar of door een subcontractant van de softwareontwikkelaar worden uitgevoerd."

BIJLAGE II

GEMEENSCHAPPELIJKE OPERATIONELE PROCEDURES (GOP) UIT HOOFDE VAN ARTIKEL 3, LID 6, VAN DE OVEREENKOMST TUSSEN DE EUROPESE UNIE EN DE ZWITSERSE BONDSSTAAT INZAKE DE KOPPELING VAN HUN REGELINGEN VOOR DE HANDEL IN BROEIKASGASEMISSIERECHTEN

Procedures voor permanente registerkoppeling

Inhoud

1. VERKLARENDE WOORDENLIJST 7
2. INLEIDING 7
2.1. Toepassingsgebied 8
2.2. Adressaten 8
3. AANPAK EN NORMEN 8
4. INCIDENTBEHEER 9
4.1. Opsporing en registratie van incidenten 9
4.2. Classificatie en initiële ondersteuning 9
4.3. Onderzoek en diagnose 10
4.4. Oplossing en herstel 10
4.5. Afsluiting van het incident 10
5. PROBLEEMBEHEER 11
5.1. Identificatie en registratie van een probleem 11
5.2. Prioritering van problemen 11
5.3. Onderzoek en diagnose van het probleem 11
5.4. Oplossing 11
5.5. Afsluiting van een probleem 11
6. AFHANDELING VAN VERZOEKEN 11
6.1. Initiatie van het verzoek 11
6.2. Registratie en analyse van het verzoek 12
6.3. Goedkeuring aanvragen 12
6.4. Afhandeling van het verzoek 12
6.5. Escalatie van een verzoek 12
6.6. Herziening van de afhandeling van het verzoek 12
6.7. Afsluiting van het verzoek 12
7. WIJZIGINGSBEHEER 12
7.1. Verzoek om wijziging 13
7.2. Evaluatie en planning van wijzigingen 13
7.3. Goedkeuring van wijzigingen 13
7.4. Implementatie van wijzigingen 13
8. RELEASEBEHEER 13
8.1. Plannen van de release 14
8.2. Bouwen en testen van releasepakket 14
8.3. Voorbereiden van uitrol 14
8.4. Terugdraaien van de release 15

8.5. Herziening en afsluiting van de release 15
9. BEHEER VAN BEVEILIGINGSINCIDENTEN 15
9.1. Categorisering van informatiebeveiligingsincidenten 15
9.2. Behandeling van informatiebeveiligingsincidenten 15
9.3. Identificatie van beveiligingsincidenten 16
9.4. Analyse van beveiligingsincidenten 16
9.5. Beoordeling van de ernst van beveiligingsincidenten, escalatie en rapportage 16
9.6. Rapportage van beveiligingsrespons 16
9.7. Monitoring, capaciteitsopbouw en continue verbetering 16
10. BEHEER VAN INFORMATIEBEVEILIGING 17
10.1. Identificatie van gevoelige informatie 17
10.2. Gevoeligheidsniveaus van de informatiebestanddelen 17
10.3. Toewijzing van de eigenaar van het informatiebestanddeel 17
10.4. Registratie van gevoelige informatie 17
10.5. Behandeling van gevoelige informatie 18
10.6. Toegangsbeheer 18
10.7. Certificaat-/sleutelbeheer 18

1. VERKLARENDE WOORDENLIJST

Tabel 1-1

Acroniemen en definities

Acroniem/term	Definitie
Certificeringsautoriteit (CA)	Entiteit die digitale certificaten uitgeeft
CH	Zwitserse Bondsstaat
ETS	Emissiehandelssysteem/emissiehandelsregeling
EU	Europese Unie
IMT	Incidentbeheerteam
Informatiebestanddeel	Informatie die waardevol is voor een bedrijf of organisatie
IT	Informatietechnologie
ITIL	Information Technology Infrastructure Library
ITSM	IT-servicebeheer
LTS	Koppelingstechnische normen
Register	Een boekhoudsysteem voor emissierechten die zijn verleend in het kader van de ETS, waarin eigendom van rechten in elektronische accounts wordt bijgehouden
RFC	Verzoek om wijziging
SIL	Lijst van gevoelige informatie
SR	Verzoek om dienstverlening
Wiki	Website waarop gebruikers informatie en kennis kunnen uitwisselen door inhoud rechtstreeks via een webbrowser aan te vullen of te wijzigen

2. INLEIDING

De Overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten van 23 november 2017 ("overeenkomst") voorziet in de wederzijdse erkenning van emissierechten die in het kader van het emissiehandelssysteem van de Europese Unie ("EU-ETS") of de emissiehandelsregeling van Zwitserland ("ETS van Zwitserland") kunnen worden gebruikt. Om de koppeling tussen het EU-ETS en de ETS van Zwitserland operationeel te maken, zal een directe koppeling tussen het EU-transactielogboek (EUTL) van het register van de Unie en het Zwitserse aanvullende transactielogboek (SSTL) van het Zwitserse register tot stand worden gebracht, waardoor onder een van beide regelingen verleende emissierechten van de ene naar de andere ETS zullen kunnen worden overgedragen (artikel 3, lid 2, van de overeenkomst). Om de koppeling tussen het EU-ETS en de ETS van Zwitserland operationeel te maken, is in 2020 een voorlopige oplossing ingevoerd. Met ingang van 2023 zal de registerkoppeling tussen de twee emissiehandelsregelingen zich geleidelijk ontwikkelen tot een permanente registerkoppeling die naar verwachting uiterlijk in 2024 tot stand zal worden gebracht en die de werking van de gekoppelde markten met betrekking tot de voordelen van marktliquiditeit en de uitvoering van transacties tussen de twee gekoppelde systemen mogelijk maakt op een wijze die gelijkwaardig is aan één markt die uit twee systemen bestaat en die marktdeelnemers in staat stelt op te treden alsof zij zich op één markt bevonden, behoudens individuele regelgeving van de partijen (bijlage II bij de overeenkomst).

Overeenkomstig artikel 3, lid 6, van de overeenkomst stellen de Zwitserse registeradministrateur en de centrale administrateur van de Unie voor technische of andere kwesties de voor de werking van de koppeling vereiste gemeenschappelijke operationele procedures vast en houden zij daarbij rekening met de prioriteiten van de nationale wetgeving. De door de administrateurs ontwikkelde GOP treden in werking wanneer zij bij besluit van het Gemengd Comité zijn vastgesteld.

De GOP zijn door het Gemengd Comité vastgesteld bij Besluit nr. 1/2020. De in dit document opgenomen geactualiseerde GOP zullen door het Gemengd Comité bij Besluit nr. 1/2024 worden vastgesteld. Overeenkomstig dat besluit en verzoeken daartoe van het Gemengd Comité hebben de Zwitserse registeradministrateur en de centrale administrateur van de Unie verdere technische richtsnoeren ontwikkeld, en zullen zij die blijven actualiseren, om de koppeling te realiseren en ervoor te zorgen dat deze voortdurend worden aangepast aan de technische vooruitgang en aan nieuwe eisen met betrekking tot de veiligheid en beveiliging van de verbinding en tot de doeltreffende en efficiënte werking ervan.

2.1. **Toepassingsgebied**

Dit document omvat het akkoord tussen de partijen bij de overeenkomst over de totstandbrenging van de procedurele grondslag van de koppeling tussen de registers van het EU-ETS en de ETS van Zwitserland. In het document worden de algemene procedurele vereisten inzake de werking van de koppeling uiteengezet. Om de koppeling te realiseren moeten echter verdere technische richtsnoeren worden vastgesteld.

Voor de goede werking van de koppeling zullen technische specificaties nodig zijn om de koppeling verder te realiseren. Overeenkomstig artikel 3, lid 7, van de overeenkomst worden deze kwesties in detail beschreven in het document betreffende koppelingstechnische normen, dat afzonderlijk bij besluit van het Gemengd Comité moet worden aangenomen.

Het doel van de GOP is ervoor te zorgen dat IT-diensten die verband houden met de werking van de koppeling tussen de registers van het EU-ETS en de ETS van Zwitserland, effectief en efficiënt worden geleverd, met name voor het inwilligen van verzoeken om dienstverlening, het oplossen van storingen en van problemen en het uitvoeren van routinetaken overeenkomstig internationale normen voor het beheer van IT-diensten.

Voor de permanente registerkoppeling zijn alleen de volgende GOP nodig, die in dit document zijn opgenomen:

— incidentbeheer,

— probleembeheer,

— afhandeling van verzoeken,

— wijzigingsbeheer,

— releasebeheer,

— beheer van beveiligingsincidenten,

— beheer van informatiebeveiliging.

2.2. **Adressaten**

De doelgroep van deze GOP zijn de teams voor ondersteuning van de registers van de EU en Zwitserland.

3. **AANPAK EN NORMEN**

Het volgende beginsel is van toepassing op alle GOP:

— de EU en CH komen overeen de GOP te definiëren op basis van ITIL (Information Technology Infrastructure Library, versie 4). De praktijken van deze norm worden hergebruikt en aangepast aan de specifieke behoeften in verband met de permanente registerkoppeling;

— de voor de verwerking van de GOP benodigde communicatie en coördinatie tussen de twee partijen vindt plaats via de servicedesks van de registers van CH en de EU. Taken worden altijd toegewezen binnen één partij;

— indien er onenigheid bestaat over de behandeling van een GOP, wordt dit geanalyseerd en tussen de beide servicedesks opgelost. Indien geen overeenstemming kan worden bereikt, wordt het vinden van een gezamenlijke oplossing geëscaleerd naar een hoger niveau:

Escalatieniveaus	EU	CH
1e niveau	EU-servicedesk	CH-servicedesk
2e niveau	Operationeel manager van de EU	Applicatiemanager van CH
3e niveau	Gemengd Comité (dat deze verantwoordelijkheid kan delegeren overeenkomstig artikel 12, lid 5, van de overeenkomst)	
4e niveau	Gemengd Comité, indien 3e niveau is gedelegeerd	

— elke partij kan de procedures voor de werking van haar eigen registratiesysteem vaststellen, rekening houdend met de eisen en interfaces van deze GOP;

— het instrument voor IT-beheer (IT Service Management, ITSM) wordt gebruikt ter ondersteuning van de GOP, met name het beheer van incidenten, het beheer van problemen en het inwilligen van verzoeken, en de communicatie tussen beide partijen;

— bovendien is de uitwisseling van informatie via e-mail toegestaan;

— beide partijen zorgen ervoor dat de voorschriften voor de beveiliging van de informatie overeenkomstig de instructies voor de behandeling ervan worden nageleefd.

4. **INCIDENTBEHEER**

Het doel van het incidentbeheerproces is om de normale werking van de IT-diensten na een incident zo snel mogelijk en met minimale verstoring te herstellen.

Incidentbeheer moet ook een register bijhouden van incidenten voor rapportagedoeleinden en met andere processen integreren om voortdurende verbetering te stimuleren.

Incidentbeheer omvat algemeen gezien de volgende activiteiten:

— opsporing en registratie van incidenten;

— classificatie en initiële ondersteuning;

— onderzoek en diagnose;

— oplossing en herstel;

— afsluiting van het incident.

Gedurende de loop van een incident is het incidentbeheer verantwoordelijk voor de eigendom, monitoring, tracering en communicatie.

4.1. **Opsporing en registratie van incidenten**

Een incident kan worden opgespoord door een ondersteuningsgroep, door geautomatiseerde monitoringinstrumenten of door technisch personeel dat routinematig toezicht uitvoert.

Na opsporing moet een incident worden geregistreerd en moet er een unieke identificatiecode worden toegewezen waarmee het incident kan worden gevolgd en gemonitord. De unieke identificatiecode van een incident is de identificatiecode die in het gemeenschappelijk ticketsysteem is toegekend door de servicedesk van de partij (EU of CH) die het incident heeft gemeld, en moet in elke communicatie over het incident worden gebruikt.

Voor alle incidenten is het contactpunt de servicedesk van de partij die het ticket heeft geregistreerd.

4.2. **Classificatie en initiële ondersteuning**

Het incident moet worden geclassificeerd om te begrijpen en te bepalen welk systeem en/of welke dienst door het incident getroffen zijn en in welke mate. Voor een doeltreffende werking moet de classificatie het incident bij de eerste poging naar de juiste dienstverlener leiden om te zorgen voor een snelle oplossing van het incident.

In de classificatiefase moeten de categorie en prioriteit van het incident worden bepaald op basis van de impact en urgentie ervan, zodat het kan worden behandeld binnen een termijn die overeenstemt met de prioriteit.

Indien het incident mogelijk gevolgen heeft voor de vertrouwelijkheid of integriteit van gevoelige gegevens en/of een impact heeft op de beschikbaarheid van het systeem, moet het incident ook worden aangemerkt als een beveiligingsincident en vervolgens worden behandeld volgens het proces dat is vastgesteld in het hoofdstuk “Beheer van beveiligingsincidenten”.

Indien mogelijk verricht de servicedesk die het ticket heeft geregistreerd een eerste diagnose. Hiervoor zal de servicedesk nagaan of het incident een bekende fout is. Als dat het geval is, is de werkwijze voor de oplossing of workaround al bekend en gedocumenteerd.

Indien de servicedesk erin slaagt het incident op te lossen, dan wordt het incident bij deze stap afgesloten, aangezien is voldaan aan het hoofddoel van het incidentbeheer (namelijk het snelle herstel van de dienst voor de eindgebruiker). Indien dit niet het geval is, escaleert de servicedesk het incident naar de desbetreffende werkgroep voor verder onderzoek en diagnose.

4.3. **Onderzoek en diagnose**

Onderzoek en diagnose van incidenten wordt toegepast wanneer een incident niet kan worden opgelost door de servicedesk als onderdeel van de initiële diagnose, en daarom wordt geëscaleerd naar het passende niveau. De escalatie van een incident maakt integraal deel uit van het onderzoeks- en diagnoseproces.

Een gangbare praktijk in de onderzoeks- en diagnosefase is te trachten om het incident onder gecontroleerde omstandigheden te reproduceren. Bij onderzoek en diagnose is het belangrijk dat een goed begrip wordt gevormd van de volgorde van de gebeurtenissen die aan het incident voorafgingen.

Escalatie is de erkenning dat een incident niet op het huidige steunniveau kan worden opgelost en moet worden doorgegeven aan een ondersteunende groep op een hoger niveau of aan de andere partij. De escalatie kan op twee manieren verlopen: horizontaal (functioneel) of verticaal (hiërarchisch).

De servicedesk die het incident heeft geregistreerd en geactiveerd, is verantwoordelijk voor het escaleren van het incident naar de juiste dienstverlener en voor het volgen van de algemene status en de toewijzing van het incident.

De partij waaraan het incident is toegewezen, is verantwoordelijk voor de tijdige uitvoering van de gevraagde maatregelen en voor het geven van feedback aan de servicedesk van de eigen partij.

4.4. **Oplossing en herstel**

De oplossing van incidenten en het herstel vindt plaats zodra een volledig begrip van het incident is gevormd. Het vinden van een oplossing voor een incident betekent dat er een manier is gevonden om het probleem te corrigeren. De handeling waarbij de oplossing wordt uitgevoerd, is de herstelfase.

Zodra de desbetreffende dienstverleners het uitvallen van de dienst hebben verholpen, wordt het incident teruggeleid naar de desbetreffende servicedesk die het incident heeft geregistreerd, en die bij de melder van het incident bevestigt dat de fout is hersteld en dat het incident kan worden afgesloten. De bevindingen van de verwerking van het incident moeten voor toekomstig gebruik worden geregistreerd.

Het herstel kan worden uitgevoerd door IT-ondersteunend personeel of door het verstrekken van een reeks instructies aan de eindgebruiker.

4.5. **Afsluiting van het incident**

Afsluiting is de laatste stap in het incidentbeheer en vindt plaats kort na de oplossing van het incident.

Van de checklist van activiteiten die tijdens de afsluitingsfase moeten worden uitgevoerd, worden de volgende activiteiten benadrukt:

— de verificatie van de initiële categorisering van het incident;

— de juiste registratie van alle informatie over het incident;

— de juiste documentatie van het incident en de bijwerking van de kennisbasis;

— de juiste communicatie met alle belanghebbenden die direct of indirect door het incident zijn getroffen.

Een incident wordt formeel gesloten zodra de fase van de afsluiting van de incidenten door de servicedesk is uitgevoerd en aan de andere partij is meegedeeld.

Zodra een incident is afgesloten, wordt het niet heropend. Als een incident zich binnen een korte periode opnieuw voordoet, wordt het oorspronkelijke incident niet opnieuw geopend, maar moet een nieuw incident worden geregistreerd.

Indien het incident wordt gevolgd door de servicedesks van zowel de EU als CH, is de definitieve afsluiting de verantwoordelijkheid van de servicedesk die het ticket heeft geregistreerd.

5. PROBLEEMBEHEER

Deze procedure moet worden gevolgd wanneer een probleem wordt vastgesteld en derhalve het proces voor probleembeheer in gang zet. Probleembeheer is gericht op het verbeteren van de kwaliteit en het verminderen van het aantal gemelde incidenten. Een probleem kan de oorzaak zijn van een of meer incidenten. Wanneer een incident wordt gemeld, is het doel van het incidentbeheer om de dienst zo snel mogelijk te herstellen, waarbij workarounds nodig kunnen zijn. Wanneer een probleem wordt geconstateerd, is het doel de onderliggende oorzaak ervan te onderzoeken om een wijziging te kunnen vaststellen die ervoor zal zorgen dat het probleem en de daarmee samenhangende incidenten niet meer zullen voorkomen.

5.1. Identificatie en registratie van een probleem

Afhankelijk van welke partij het ticket heeft geopend, is de servicedesk van de EU of CH het contactpunt voor alle aan het probleem gerelateerde kwesties.

De unieke identificatiecode van een probleem is de identificatiecode die door het ITSM wordt toegekend. De code moet worden gebruikt in alle communicatie in verband met het probleem.

Een probleem kan worden geactiveerd door een incident, of kan op eigen initiatief worden geopend om een oplossing te vinden voor problemen die op eender welk ogenblik in het systeem worden geconstateerd.

5.2. Prioritering van problemen

Problemen kunnen op dezelfde wijze als incidenten worden gecategoriseerd op basis van de ernst en prioriteit ervan, om het volgen ervan te vergemakkelijken, rekening houdend met de gevolgen van de betrokken incidenten en de frequentie waarmee zij zich hebben voorgedaan.

5.3. Onderzoek en diagnose van het probleem

Elke partij kan een probleem melden, waarna de servicedesk van de desbetreffende partij verantwoordelijk is voor de registratie ervan, de toewijzing ervan aan de juiste dienstverlener, en het volgen van de algemene status ervan.

Het oplossingsteam waaraan het probleem is geëscaleerd, is verantwoordelijk voor het tijdig behandelen van het probleem en voor de communicatie met de servicedesk.

Na een verzoek zijn beide partijen verantwoordelijk voor de uitvoering van de toegewezen acties en voor het geven van feedback aan de servicedesk van de eigen partij.

5.4. Oplossing

Het oplossingsteam waaraan het probleem is toegewezen, is verantwoordelijk voor het oplossen van het probleem en het verstrekken van relevante informatie aan de servicedesk van de eigen partij.

De bevindingen van de verwerking van het probleem moeten voor toekomstig gebruik worden geregistreerd.

5.5. Afsluiting van een probleem

Een probleem wordt formeel afgesloten zodra het probleem is opgelost door de wijziging door te voeren. De afsluitingsfase wordt uitgevoerd door de servicedesk die het probleem heeft geregistreerd en de servicedesk van de andere partij daarvan in kennis heeft gesteld.

6. AFHANDELING VAN VERZOEKEN

De afhandeling van verzoeken omvat het volledige beheer van een verzoek om een nieuwe of bestaande dienst vanaf het moment dat het is geregistreerd en goedgekeurd tot aan de afsluiting ervan. Het gaat meestal om kleine, vooraf gedefinieerde, herhaalbare, frequente, vooraf goedgekeurde en procedurele verzoeken.

Hieronder volgt een overzicht van de belangrijkste stappen die moeten worden ondernomen.

6.1. Initiatie van het verzoek

De informatie met betrekking tot een verzoek om dienstverlening wordt per e-mail, per telefoon, of via het ITSM of een ander overeengekomen communicatiekanaal bij de servicedesk van de EU of CH ingediend.

6.2. **Registratie en analyse van het verzoek**

Voor alle verzoeken om dienstverlening moet het contactpunt de EU- of CH-servicedesk zijn, afhankelijk van welke partij het verzoek heeft ingediend. Deze servicedesk is verantwoordelijk voor het bijhouden en analyseren van het verzoek om dienstverlening en de passende zorgvuldigheid.

6.3. **Goedkeuring aanvragen**

De medewerker van de servicedesk van de partij die het verzoek om dienstverlening heeft ingediend, controleert of er goedkeuring van de andere partij nodig is, en zo ja, verkrijgt deze. Indien het verzoek om dienstverlening niet wordt goedgekeurd, wordt het ticket door de servicedesk geactualiseerd en afgesloten.

6.4. **Afhandeling van het verzoek**

Deze stap is gericht op een doeltreffende en efficiënte afhandeling van de verzoeken om dienstverlening. Hierbij worden de volgende categorieën gehanteerd:

— de afhandeling van het verzoek om dienstverlening heeft voor slechts één partij gevolgen. In dit geval geeft deze partij de werkopdrachten en coördineert zij de uitvoering;

— de afhandeling van het verzoek om dienstverlening heeft gevolgen voor zowel EU als CH. In dit geval geven de servicedesks van de werkopdrachten op hun bevoegdheidsgebied. De verwerking van de afhandeling van het verzoek om dienstverlening wordt tussen beide servicedesks gecoördineerd. De algemene verantwoordelijkheid ligt bij de servicedesk die het verzoek heeft ontvangen en geïnitieerd.

Wanneer het verzoek om dienstverlening is afgehandeld, moet het de status “Opgelost” worden gegeven.

6.5. **Escalatie van een verzoek**

De servicedesk kan het lopende verzoek om dienstverlening, indien nodig, naar de juiste dienstverlener escaleren (derde partij).

Escalaties worden uitgevoerd aan de respectieve derde partijen, dat wil zeggen dat de EU-servicedesk via de CH-servicedesk voor escalatie naar een derde CH-partij zal moeten gaan, en omgekeerd.

De derde partij waaraan het verzoek geëscaleerd is, is verantwoordelijk voor de tijdige behandeling van het verzoek en voor de communicatie met de servicedesk die het verzoek heeft geëscaleerd.

De servicedesk die het verzoek om dienstverlening heeft aangemeld, is verantwoordelijk voor het traceren van de algemene status en de toewijzing van een verzoek om dienstverlening.

6.6. **Herziening van de afhandeling van het verzoek**

De verantwoordelijke servicedesk onderwerpt de over het verzoek om dienstverlening geregistreerde gegevens aan een laatste kwaliteitscontrole voordat het wordt afgesloten. Het doel daarvan is om er zeker van te zijn dat een verzoek om dienstverlening daadwerkelijk wordt verwerkt en dat alle informatie die nodig is om de levenscyclus van het verzoek te beschrijven, voldoende gedetailleerd wordt verstrekt. Daarnaast moeten de bevindingen van de verwerking van het verzoek worden geregistreerd voor toekomstig gebruik.

6.7. **Afsluiting van het verzoek**

Indien de aangewezen partijen overeenkomen dat het verzoek om dienstverlening is ingewilligd en de verzoeker van mening is dat de zaak is opgelost, wordt de status veranderd in “Afgesloten”.

Een verzoek om dienstverlening is formeel afgesloten zodra de servicedesk die het dienstverzoek heeft geregistreerd, de afsluitingsfase heeft uitgevoerd en de servicedesk van de andere partij daarvan in kennis heeft gesteld.

7. **WIJZIGINGSBEHEER**

Het doel is ervoor te zorgen dat gestandaardiseerde methoden en procedures worden gebruikt voor een efficiënte en snelle afhandeling van alle wijzigingen van de IT-infrastructuur, teneinde het aantal van eventuele gerelateerde incidenten en de gevolgen daarvan voor de dienstverlening tot een minimum te beperken. Wijzigingen in de IT-infrastructuur kunnen zich voordoen als reactie op problemen of extern opgelegde vereisten, bijvoorbeeld wijzigingen van de wetgeving, of proactief met het oog op meer efficiëntie en doeltreffendheid of om zakelijke initiatieven mogelijk te maken of te weerspiegelen.

Het wijzigingsbeheer omvat verschillende stappen die alle details van een wijzigingsverzoek opslaan voor toekomstige tracering. Die processen zorgen ervoor dat de wijziging gevalideerd en getest wordt alvorens te worden doorgevoerd. Releasebeheer is verantwoordelijk voor de succesvolle uitrol van de wijziging.

7.1. **Verzoek om wijziging**

Een verzoek om wijziging (RFC) wordt ter validering en goedkeuring ingediend bij het wijzigingsbeheerteam. Voor alle wijzigingsverzoeken moet het contactpunt de EU- of CH-servicedesk zijn, afhankelijk van welke partij het verzoek heeft ingediend. Deze servicedesk is verantwoordelijk voor het registreren en analyseren van het verzoek met de nodige zorgvuldigheid.

Wijzigingsverzoeken kunnen voortkomen uit:

— een incident dat een wijziging veroorzaakt;

— een bestaand probleem dat tot een wijziging leidt;

— een eindgebruiker die een nieuwe wijziging verzoekt;

— een wijziging als gevolg van lopend onderhoud;

— wijzigingen in de wetgeving.

7.2. **Evaluatie en planning van wijzigingen**

In deze fase worden de beoordelings- en planningsactiviteiten behandeld. De fase omvat prioritering en planningsactiviteiten om de risico's en de impact tot een minimum te beperken.

Indien de uitvoering van het wijzigingsverzoek gevolgen heeft voor zowel de EU als CH, verifieert de partij die het verzoek heeft aangemeld, de evaluatie en planning van de wijziging met de andere partij.

7.3. **Goedkeuring van wijzigingen**

Elk geregistreerd wijzigingsverzoek moet door het desbetreffende escalatieniveau worden goedgekeurd.

7.4. **Implementatie van wijzigingen**

De wijzigingen worden geïmplementeerd via het releasebeheerproces. De releasebeheerteams van beide partijen volgen hun eigen processen met betrekking tot planning en tests. Herziening vindt plaats zodra de implementatie is voltooid. Om er zeker van te zijn dat alles volgens plan is verlopen, wordt het bestaande proces van wijzigingsbeheer voortdurend geëvalueerd en waar nodig geactualiseerd.

8. **RELEASEBEHEER**

Onder release wordt een of meer wijzigingen in een IT-dienst verstaan die worden verzameld in een releaseplan, en samen worden goedgekeurd, voorbereid, gebouwd, getest en uitgerold. Een release kan de oplossing van een bug omvatten, of een wijziging van de hardware of andere onderdelen, wijziging van de software, upgrades van applicaties, wijzigingen van de documentatie en/of processen. De inhoud van elke release wordt als een enkele entiteit beheerd, getest en uitgerold.

Releasebeheer is gericht op het plannen, bouwen, testen en valideren van en het leveren van de capaciteit voor het verlenen van de diensten, die de eisen van de belanghebbenden zullen vervullen en de beoogde doelstellingen zullen verwezenlijken. De acceptatiecriteria voor alle wijzigingen van de dienst zullen worden vastgesteld en gedocumenteerd bij de coördinatie van het ontwerp en worden verstrekt aan de releasebeheerteams.

Een release bestaat doorgaans uit een aantal oplossingen van problemen en verbeteringen van een dienst. Hij omvat de vereiste nieuwe of veranderde software en de nieuwe of veranderde hardware die nodig is om de goedgekeurde wijzigingen uit te voeren.

8.1. **Plannen van de release**

In de eerste stap van het proces worden geautoriseerde wijzigingen aan releasepakketten toegewezen en worden het toepassingsgebied en de inhoud van de releases bepaald. Op basis van deze informatie ontwikkelt het subproces van de releaseplanning een tijdschema voor de opbouw, het testen en het uitrollen van de release.

Bij de planning moet het volgende worden bepaald:

— toepassingsgebied en inhoud van de release;

— risicobeoordeling en risicoprofiel voor de release;

— de door de release getroffen klant/gebruikers;

— team dat verantwoordelijk is voor de release;

— strategie voor levering en uitrol;

— middelen voor de release en de uitrol ervan.

Beide partijen brengen elkaar op de hoogte van de planning van releases en onderhoudsvensters. Indien een release gevolgen heeft voor zowel de EU als CH, coördineren zij de planning en stellen zij een gemeenschappelijk onderhoudsvenster vast.

8.2. **Bouwen en testen van releasepakket**

Bij de bouw- en teststap van het releasebeheerproces wordt de benadering vastgesteld van de uitvoering van de release of het releasepakket en van de handhaving van de gecontroleerde omgeving voorafgaand aan de wijziging van de productie, alsmede het testen van alle wijzigingen van de release in alle omgevingen.

Indien een release gevolgen heeft voor zowel de EU als CH, coördineren zij de releaseplanning en de tests. Hierbij komen de volgende aspecten aan bod:

— hoe en wanneer release-units en dienstencomponenten zullen worden geleverd;

— wat de typische aanlooptijd is; wat er gebeurt in geval van een vertraging;

— hoe de voortgang van de levering wordt bijgehouden en bevestiging wordt verkregen;

— maatstaven voor monitoring en bepaling van het succes van de uitrol van de release;

— gemeenschappelijke testcases voor relevante functies en wijzigingen.

Aan het eind van dit subproces zijn alle voorgeschreven onderdelen klaar voor de uitrolfase.

8.3. **Voorbereiden van uitrol**

Door het voorbereidingssubproces wordt gewaarborgd dat de communicatieplannen correct zijn gedefinieerd en de kennisgevingen klaar zijn om te worden toegezonden aan alle belanghebbenden en eindgebruikers, en dat de release wordt geïntegreerd in het proces van wijzigingsbeheer om ervoor te zorgen dat alle wijzigingen op een gecontroleerde manier worden uitgevoerd en door de vereiste fora worden goedgekeurd.

Indien een release gevolgen heeft voor zowel de EU als CH, coördineren zij de volgende activiteiten:

— wijzigingsaanvragen registreren voor planning en voorbereiding van uitrol in de productieomgeving;

— opstellen van het uitvoeringsplan;

— een aanpak voor eventuele terugdraaiing, zodat in geval van een mislukte uitrol terug kan worden gekeerd naar de vorige staat;

— kennisgevingen die aan alle noodzakelijke partijen worden gezonden;

— goedkeuring vragen voor de uitvoering van de release van het desbetreffende escalatieniveau.

8.4. **Terugdraaien van de release**

Indien de uitrol is mislukt of indien bij de tests is geconstateerd dat de uitrol niet succesvol is of niet voldoet aan de vastgestelde acceptatie- of kwaliteitscriteria, dan moeten de releasebeheerteams van beide partijen de uitrol terugdraaien. Alle noodzakelijke belanghebbenden moeten worden geïnformeerd, met inbegrip van de getroffen/beoogde eindgebruikers. In afwachting van goedkeuring kan het proces in elk van de vorige fasen opnieuw worden gestart.

8.5. **Herziening en afsluiting van de release**

Bij de herziening van een uitrol moeten de volgende activiteiten worden opgenomen:

— verzamelen van feedback over de tevredenheid van klanten, gebruikers en diensten met de uitrol (verzamelen en bestuderen van de feedback voor de voortdurende verbetering van de dienst);

— herzien van de kwaliteitscriteria waaraan niet is voldaan;

— controleren of alle maatregelen, noodzakelijke correcties en de wijzigingen zijn afgerond;

— ervoor zorgen dat er aan het einde van de uitrol geen problemen op het gebied van capaciteit, middelen of prestaties zijn;

— verifiëren dat eventuele problemen, bekende fouten en workarounds worden gedocumenteerd en aanvaard door de klant, de eindgebruikers, de operationele ondersteuning en andere betrokken partijen;

— toezicht houden op incidenten en problemen die het gevolg zijn van de uitrol (het verlenen van steun in de beginfase aan operationele teams indien de release leidt tot een toename van de hoeveelheid werk);

— bijwerken van de ondersteunende documentatie (d.w.z. technische informatiedocumenten);

— de uitrol van de release formeel overdragen aan de operationele teams;

— documentatie van geleerde lessen;

— documenten met de samenvatting van de release van de uitvoerende teams verzamelen;

— de release formeel afsluiten na de controle van de registratie van het wijzigingsverzoek.

9. **BEHEER VAN BEVEILIGINGSINCIDENTEN**

Beheer van beveiligingsincidenten is een proces voor de behandeling van beveiligingsincidenten om de belanghebbenden in staat te stellen informatie over incidenten te verstrekken; evaluatie en prioritering van incidenten, en incidentrespons om een feitelijke, vermeende of mogelijke inbreuk op de vertrouwelijkheid, beschikbaarheid of integriteit van gevoelige informatie te regelen.

9.1. **Categorisering van informatiebeveiligingsincidenten**

Alle incidenten die van invloed zijn op de koppeling tussen het register van de Unie en het Zwitserse register worden geanalyseerd om een mogelijke inbreuk op de vertrouwelijkheid, de integriteit of de beschikbaarheid van gevoelige informatie op de Lijst van gevoelige informatie (SIL) vast te stellen.

Als dat het geval is, moet het incident worden aangemerkt als een incident op het gebied van informatiebeveiliging, onmiddellijk worden geregistreerd in het ITSM en als zodanig worden beheerd.

9.2. **Behandeling van informatiebeveiligingsincidenten**

Beveiligingsincidenten vallen onder de verantwoordelijkheid van het 3e escalatieniveau en de oplossing van de incidenten wordt behandeld door een specifiek team voor incidentbeheer (IMT).

Het IMT is verantwoordelijk voor:

— het uitvoeren van een eerste analyse en het categoriseren en beoordelen van de ernst van het incident;

— het coördineren van acties tussen alle belanghebbenden, met inbegrip van de volledige documentatie van de analyse van het incident, de besluiten die zijn genomen om het incident aan te pakken en de mogelijke vastgestelde tekortkomingen;

— afhankelijk van de ernst van het beveiligingsincident, de tijdige escalatie van het incident naar het juiste niveau voor informatie en/of een beslissing.

Bij het beheer van informatiebeveiliging wordt alle informatie betreffende incidenten gerubriceerd op het hoogste niveau van gevoeligheid van de informatie, maar in elk geval niet lager dan SENSITIVE: *ETS*.

Voor een lopend onderzoek en/of een tekortkoming die kan worden misbruikt en tot aan het herstel ervan, wordt de informatie gerubriceerd als SPECIAL HANDLING: *ETS Critical*.

9.3. **Identificatie van beveiligingsincidenten**

De informatiebeveiligingsfunctionaris bepaalt op basis van aard van het incident de passende organisaties die moeten worden betrokken en deel moeten uitmaken van het IMT.

9.4. **Analyse van beveiligingsincidenten**

Het IMT werkt samen met alle betrokken organisaties en de betrokken leden van hun teams, naargelang van het geval, bij de beoordeling van het incident. Tijdens de analyse wordt de mate van het verlies van vertrouwelijkheid, integriteit of beschikbaarheid vastgesteld en worden de gevolgen voor alle betrokken organisaties beoordeeld. Vervolgens worden initiële en follow-upacties vastgesteld om het incident op te lossen en de gevolgen ervan te beheren, met inbegrip van het effect van die maatregelen op de middelen.

9.5. **Beoordeling van de ernst van beveiligingsincidenten, escalatie en rapportage**

Het IMT beoordeelt de ernst van elk nieuw beveiligingsincident na de categorisering ervan als beveiligingsincident en begint met onmiddellijke maatregelen naargelang de ernst van het incident.

9.6. **Rapportage van beveiligingsrespons**

Het IMT vermeldt de resultaten van de beperking en het herstel van het incident in het incidentresponsverslag. Het verslag wordt aan het 3e escalatieniveau verstrekt door middel van beveiligde e-mail of andere wederzijds aanvaarde middelen van beveiligde communicatie.

De verantwoordelijke partij evalueert de resultaten van de beperking en het herstel en:

— verbindt het register opnieuw indien de verbinding eerder was verbroken;

— verstrekt incidentmeldingen aan de teams van het register;

— sluit het incident af.

Het IMT moet — op een veilige manier — relevante details vermelden in het verslag over het informatiebeveiligingsincident, teneinde een consistente registratie en communicatie te waarborgen en een snelle en passende actie mogelijk te maken om het incident te beperken. Het IMT dient het eindverslag over het informatiebeveiligingsincident na voltooiing te zijner tijd in.

9.7. **Monitoring, capaciteitsopbouw en continue verbetering**

Het IMT brengt voor alle beveiligingsincidenten verslag uit aan het 3e escalatieniveau. De verslagen zullen door dit escalatieniveau worden gebruikt om het volgende te bepalen:

— zwakke punten in de beveiligingscontroles en/of de functionering die moeten worden versterkt;

— een mogelijke behoefte om deze procedure te versterken om de doeltreffendheid van de respons op incidenten te verbeteren;

— opleiding en capaciteitsopbouw om de informatiebeveiliging van registersystemen verder te versterken, het risico op toekomstige incidenten te verminderen en het effect ervan tot een minimum te beperken.

10. **BEHEER VAN INFORMATIEBEVEILIGING**

Beheer van informatiebeveiliging heeft ten doel de vertrouwelijkheid, integriteit en beschikbaarheid van de gerubriceerde informatie, gegevens en IT-diensten van een organisatie te waarborgen. Naast de technische onderdelen, met inbegrip van het ontwerp en de tests (zie LTS), zijn de volgende gemeenschappelijke operationele procedures nodig om aan de beveiligingseisen voor de permanente registerkoppeling te voldoen.

10.1. **Identificatie van gevoelige informatie**

De gevoeligheid van informatie wordt beoordeeld aan de hand van de gevolgen voor het bedrijf (bv. Financiële verliezen, reputatieschade, schending van het recht …) die een beveiligingsinbreuk in verband met de informatie zou kunnen hebben.

De gevoeligheid van informatie wordt bepaald op basis van het effect ervan op de koppeling.

Het gevoeligheidsniveau van deze informatie wordt beoordeeld aan de hand van de gevoeligheidsschaal die van toepassing is op deze koppeling en nader uitgewerkt in het gedeelte “Behandeling van informatiebeveiligingsincidenten” van dit document.

10.2. **Gevoeligheidsniveaus van de informatiebestanddelen**

Bij de identificatie wordt een informatiebestanddeel gerubriceerd aan de hand van de volgende regels:

— bij de identificatie van ten minste één HOOG vertrouwelijkheids-, integriteits- of beschikbaarheidsniveau wordt het informatiebestanddeel gerubriceerd als SPECIAL HANDLING: *ETS Critical*;

— bij de identificatie van ten minste één MIDDELHOOG vertrouwelijkheids-, integriteits- of beschikbaarheidsniveau wordt het informatiebestanddeel gerubriceerd als SENSITIVE: *ETS*;

— bij de identificatie van ten minste één LAAG vertrouwelijkheids-, integriteits- of beschikbaarheidsniveau wordt het informatiebestanddeel gerubriceerd als Marking EU: SENSITIVE: *ETS Joint Procurement;* Marking CH: LIMITED: *ETS*.

10.3. **Toewijzing van de eigenaar van het informatiebestanddeel**

Alle informatiebestanddelen moeten een toegewezen eigenaar hebben. Informatiebestanddelen van de ETS, die behoren tot of verband houden met de koppeling tussen het EUTL en het SSTL, moeten worden opgenomen in een gezamenlijke inventaris van informatiebestanddelen, die door beide partijen wordt bijgehouden. Informatiebestanddelen van de ETS buiten de koppeling tussen het EUTL en het SSTL moeten worden opgenomen in een inventaris van de bestanddelen, die door de respectieve partij wordt bijgehouden.

De eigendom van elk informatiebestanddeel dat behoort tot of verband houdt met de koppeling tussen het EUTL en de SSTL moet worden overeengekomen door de partijen. De eigenaar van een informatiebestanddeel is verantwoordelijk voor de beoordeling van de gevoeligheid ervan.

De eigenaar moet een anciënniteit hebben die passend is voor de waarde van het toegewezen bestanddeel/de toegewezen bestanddelen. De verantwoordelijkheid van de eigenaar voor het bestanddeel/de bestanddelen en diens verplichting om het vereiste niveau van vertrouwelijkheid, integriteit en beschikbaarheid te handhaven, moet worden overeengekomen en geformaliseerd.

10.4. **Registratie van gevoelige informatie**

Alle gevoelige informatie wordt geregistreerd in de Lijst voor gevoelige informatie (SIL).

In voorkomend geval wordt de samenvoeging van gevoelige informatie die tot een groter effect zou kunnen leiden dan het effect van één enkel informatiebestanddeel, in aanmerking genomen en geregistreerd in de SIL (bv. een verzameling van informatie die in de systeemdatabank is opgeslagen).

De SIL is niet statisch. Dreigingen, kwetsbaarheden en de waarschijnlijkheid of gevolgen van beveiligingsincidenten met betrekking tot de informatie kunnen zonder enige indicatie veranderen en nieuwe informatiebestanddelen kunnen worden opgenomen in de registersystemen.

De SIL wordt derhalve regelmatig geëvalueerd en alle nieuwe als gevoelig aangemerkte informatie wordt onmiddellijk in de SIL geregistreerd.

De SIL bevat voor elke vermelding ten minste de volgende gegevens:

— beschrijving van de informatie;

— eigenaar van de informatie;

— gevoeligheidsniveau;

— vermelding of de informatie persoonsgegevens bevat;

— aanvullende informatie, indien nodig.

10.5. **Behandeling van gevoelige informatie**

Wanneer gevoelige informatie buiten de koppeling tussen het register van de Unie en het Zwitserse register wordt verwerkt, wordt deze behandeld overeenkomstig de instructies voor de behandeling van gevoelige informatie.

Gevoelige informatie die wordt verwerkt door de koppeling tussen het register van de Unie en het Zwitserse register wordt behandeld overeenkomstig de beveiligingsvoorschriften van de partijen.

10.6. **Toegangsbeheer**

Het doel van het toegangsbeheer is geautoriseerde gebruikers het recht te geven gebruik te maken van een dienst, waarbij de toegang voor niet-geautoriseerde gebruikers wordt verhinderd. Toegangsbeheer wordt soms ook “rechtenbeheer” of “identiteitsbeheer” genoemd.

Voor de permanente registerkoppeling en de werking ervan hebben beide partijen toegang nodig tot:

— wiki: een samenwerkingsomgeving voor de uitwisseling van gemeenschappelijke informatie, zoals releaseplanning;

— het ITSM voor het beheer van incidenten en problemen (zie hoofdstuk 3 “Aanpak en normen”);

— een systeem voor de uitwisseling van berichten: elke partij voorziet in een beveiligd systeem voor de uitwisseling van berichten waarin de transactiegegevens worden doorgegeven.

De Zwitserse registeradministrateur en de centrale administrateur van de Unie zien erop toe dat de toegangen beschikbaar zijn en fungeren als contactpunten voor hun partijen voor activiteiten op het gebied van toegangsbeheer. Verzoeken om toegang worden behandeld volgens de procedures voor het afhandelen van verzoeken.

10.7. **Certificaat-/sleutelbeheer**

Elke partij is verantwoordelijk voor haar eigen certificaat-/sleutelbeheer (productie, registratie, opslag, installatie, gebruik, verlenging, intrekking, backup en recuperatie van certificaten/sleutels). Zoals uiteengezet in de koppelingstechnische normen (LTS), worden alleen digitale certificaten gebruikt die zijn afgegeven door een door beide partijen vertrouwde certificeringsautoriteit (CA). Bij de behandeling en opslag van certificaten/sleutels moeten de bepalingen van de instructies voor de behandeling worden gevolgd.

De intrekking en/of verlenging van certificaten en sleutels moet altijd door beide partijen gecoördineerd. Dit gebeurt volgens de procedures voor het afhandelen van verzoeken.

De Zwitserse registeradministrateur en de centrale administrateur van de Unie zullen certificaten/sleutels uitwisselen via beveiligde communicatiemiddelen overeenkomstig de instructies in de instructies voor behandeling.

Eventuele verificatie van certificaten/sleutels tussen de partijen vindt plaats buiten de band.

BIJLAGE III

KOPPELINGSTECHNISCHE NORMEN (LTS) UIT HOOFDE VAN ARTIKEL 3, LID 7, VAN DE OVEREENKOMST TUSSEN DE EUROPESE UNIE EN DE ZWITSERSE BONDSSTAAT INZAKE DE KOPPELING VAN HUN REGELINGEN VOOR DE HANDEL IN BROEIKASGASEMISSIERECHTEN

Normen voor permanente registerkoppeling

Inhoud

1. VERKLARENDE WOORDENLIJST 21
2. INLEIDING 22
2.1. Toepassingsgebied 22
2.2. Adressaten 23
3. ALGEMENE BEPALINGEN 23
3.1. Architectuur van de communicatiekoppeling 23
3.1.1. Uitwisseling van berichten 23
3.1.2. XML-bericht — Beschrijving op hoog niveau 23
3.1.3. Opnamevensters 24
3.1.4. Transactieberichtenstroom 24
3.2. Beveiliging van gegevensoverdracht 26
3.2.1. Firewall en netwerkinterconnectie 26
3.2.2. Virtueel particulier netwerk (VPN) 26
3.2.3. Uitvoering van IPSec 27
3.2.4. Overdrachtprotocol voor beveiligde uitwisseling van berichten 27
3.2.5. XML-versleuteling en -ondertekening 27
3.2.6. Cryptografische sleutels 27
3.3. Lijst van functies in het kader van de koppeling 27
3.3.1. Zakelijke transacties 28
3.3.2. Afstemmingsprotocol 28
3.3.3. Testbericht 28
3.4. Vereisten voor gegevensregistratie 29
3.5. Operationele vereisten 29
4. BESCHIKBAARHEIDSBEPALINGEN 30
4.1. Ontwerp voor de beschikbaarheid van de communicatie 30
4.2. Initialisatie, communicatie, heractivering en testplan 30
4.2.1. Interne tests van de ICT-infrastructuur 31
4.2.2. Communicatietests 31
4.2.3. Volledige systeemtest (eind-tot-eind) 31
4.2.4. Beveiligingstests 31
4.3. Acceptatie-/testomgevingen 32
5. BEPALINGEN INZAKE VERTROUWELIJKHEID EN INTEGRITEIT 32
5.1. Infrastructuur voor beveiligingstests 32
5.2 Onderbreking van de koppeling en bepalingen betreffende heractivering 32
5.3. Bepalingen inzake beveiligingsinbreuk 33

5.4. Richtsnoeren voor het testen van de beveiliging 33
5.4.1. Programmatuur 33
5.4.2. Infrastructuur 34
5.5. Bepalingen inzake risicobeoordeling 34

1. **VERKLARENDE WOORDENLIJST**

Tabel 1-1

Bedrijfsacroniemen en definities

Acroniem/term	Definitie
CH	Zwitserse Bondsstaat.
CHU	Type emissierechten voor stationaire installaties, ook wel CHU2 genoemd (verwijzend naar vastleggingsperiode 2 van het Protocol van Kyoto), afgegeven door CH.
CHUA	Emissierechten van de Zwitserse luchtvaart.
Emissierecht	Een emissierecht om gedurende een bepaalde periode één ton kooldioxide-equivalent uit te stoten, dat alleen geldig is om te voldoen aan de vereisten van de ETS van een van beide entiteiten.
ETR	Emissiehandelsregister.
ETS	Emissiehandelssysteem/emissiehandelsregeling.
EU	Europese Unie.
EUA	Algemene emissierechten van de EU.
EUAA	Luchtvaartemissierechten van de EU.
EUCR	Geconsolideerd register van de Europese Unie.
EUTL	EU-transactielogboek.
GOP	Gemeenschappelijke operationele procedures. Gemeenschappelijk ontwikkelde procedures om de koppeling tussen het EU-ETS en de ETS van Zwitserland te realiseren.
Register	Een boekhoudsysteem voor emissierechten die zijn verleend in het kader van de ETS, waarin eigendom van rechten in elektronische accounts wordt bijgehouden.
SSTL	Zwitsers aanvullend transactielogboek.
Transactie	Een proces in een register waarbij een emissierecht van een rekening naar een andere rekening wordt overgedragen.
Transactielogboek	Het transactielogboek bevat een register van elke voorgestelde transactie die van het ene register naar het andere wordt verzonden.

Tabel 1-2

Technische acroniemen en definities

Acroniem	Definitie
Afstemmingsproces	Proces om ervoor te zorgen dat twee reeksen gegevens met elkaar overeenstemmen.
Asymmetrische cryptografie	Maakt gebruik van publieke en private sleutels voor het versleutelen en ontsleutelen van gegevens.
Bestandopname	Het proces waarbij een bestand wordt gelezen.
Buffer	Apparatuur of software voor netwerkbeveiliging die het inkomende en uitgaande netwerkverkeer monitort en controleert op basis van vooraf vastgestelde regels.
Certificeringsautoriteit (CA)	Entiteit die digitale certificaten uitgeeft.
Cryptografische sleutel	Een stuk informatie dat de functionele output van een cryptografisch algoritme bepaalt.
Digitale handtekening	Een mathematische techniek die wordt gebruikt om de authenticiteit en integriteit van een bericht, software of een digitaal document te valideren.

Acroniem	Definitie
Heartbeatmonitoring	Periodiek door hardware of software gegenereerd en bewaakt signaal om de normale werking aan te geven of om andere delen van een computersysteem te synchroniseren.
IPSec	IP SECurity (IP-beveiliging), netwerkprotocolsuite die de gegevenspakketten authenticeert en versleutelt om te zorgen voor een beveiligde, versleutelde communicatie tussen twee computers over een internetprotocolnetwerk.
Ontsleuteling	Omgekeerd proces van versleuteling.
Penetratietest	Praktijk van het testen van een computersysteem, netwerk of webtoepassing om beveiligingskwetsbaarheden op te sporen die een aanvaller zou kunnen benutten.
Versleuteling	Het omzetten van informatie of gegevens in een code, met name om ongeoorloofde toegang te voorkomen.
VPN	Virtueel particulier netwerk.
XML	Extensible Mark-up Language. Biedt ontwerpers de mogelijkheid om hun eigen specifieke tags te creëren, waardoor de gegevens tussen de verschillende toepassingen en tussen de verschillende organisaties kunnen worden gedefinieerd, verzonden, gevalideerd en geïnterpreteerd.

2. **INLEIDING**

De Overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten van 23 november 2017 ("overeenkomst") voorziet in de wederzijdse erkenning van emissierechten die in het kader van het emissiehandelssysteem van de Europese Unie ("EU-ETS") of de emissiehandelsregeling van Zwitserland ("ETS van Zwitserland") kunnen worden gebruikt. Om de koppeling tussen het EU-ETS en de ETS van Zwitserland operationeel te maken, zal een directe koppeling tussen het EU-transactielogboek (EUTL) van het register van de Unie en het Zwitserse aanvullende transactielogboek (SSTL) van het Zwitserse register tot stand worden gebracht, waardoor onder een van beide regelingen verleende emissierechten van de ene naar de andere ETS zullen kunnen worden overgedragen (artikel 3, lid 2, van de overeenkomst). Om de koppeling tussen het EU-ETS en de ETS van Zwitserland operationeel te maken, is in 2020 een voorlopige oplossing ingevoerd. Met ingang van 2023 zal de registerkoppeling tussen de twee emissiehandelsregelingen zich geleidelijk ontwikkelen tot een permanente registerkoppeling die naar verwachting uiterlijk in 2024 tot stand zal worden gebracht en die de werking van de gekoppelde markten met betrekking tot de voordelen van marktliquiditeit en de uitvoering van transacties tussen de twee gekoppelde systemen mogelijk maakt op een wijze die gelijkwaardig is aan één markt die uit twee systemen bestaat en die marktdeelnemers in staat stelt op te treden alsof zij zich op één markt bevonden, behoudens individuele regelgeving van de partijen (bijlage II bij de overeenkomst).

Overeenkomstig artikel 3, lid 7, van de Overeenkomst stellen de Zwitserse registeradministrateur en de centrale administrateur van de Unie op basis van de beginselen in bijlage II bij de overeenkomst koppelingstechnische normen vast waarin de gedetailleerde eisen voor het tot stand brengen van een robuuste en veilige verbinding tussen het SSTL en het EUTL worden beschreven. De door de administrateurs ontwikkelde koppelingstechnische normen treden in werking wanneer zij bij besluit van het Gemengd Comité zijn aangenomen.

De LTS zijn door het Gemengd Comité vastgesteld bij Besluit nr. 2/2020. De in dit document opgenomen geactualiseerde LTS zullen door het Gemengd Comité bij Besluit nr. 1/2024 worden vastgesteld. Overeenkomstig dat besluit en verzoeken daartoe van het Gemengd Comité hebben de Zwitserse registeradministrateur en de centrale administrateur van de Unie verdere technische richtsnoeren ontwikkeld, en zullen zij die blijven actualiseren, om de koppeling te realiseren en ervoor te zorgen dat die voortdurend worden aangepast aan de technische vooruitgang en aan nieuwe eisen met betrekking tot de veiligheid en beveiliging van de verbinding en tot de doeltreffende en efficiënte werking ervan.

2.1. **Toepassingsgebied**

Dit document omvat het akkoord tussen de partijen bij de overeenkomst over de totstandbrenging van de technische grondslag van de koppeling tussen de registers van het EU-ETS en de ETS van Zwitserland. Dit document vormt de basis voor de technische specificaties met betrekking tot eisen op het gebied van architectuur, dienstverlening en beveiliging, maar enkele verdere gedetailleerde richtsnoeren zijn nodig om de koppeling operationeel te maken.

Voor de goede werking van de koppeling zullen processen en procedures nodig zijn om haar verder te realiseren. Op grond van artikel 3, lid 6, van de overeenkomst worden die kwesties in detail beschreven in een apart document betreffende gemeenschappelijke operationele procedures (GOP), dat afzonderlijk bij besluit van het Gemengd Comité moet worden aangenomen.

2.2. **Adressaten**

Dit document is gericht tot de Zwitserse registeradministrateur en de centrale administrateur van de Unie.

3. **ALGEMENE BEPALINGEN**

3.1. **Architectuur van de communicatiekoppeling**

Het doel van dit hoofdstuk is een beschrijving te geven van de algemene architectuur van de realisering van de koppeling tussen het EU-ETS en de ETS van Zwitserland en de verschillende onderdelen ervan.

Beveiliging is een essentieel onderdeel van de robuuste architectuur van de registerkoppeling, en daartoe zijn alle nodige maatregelen genomen. De permanente registerkoppeling maakt gebruik van een mechanisme voor de uitwisseling van bestanden, als implementatie van een beveiligde airgapverbinding.

Voor de technische oplossing wordt gebruikgemaakt van:

— een beveiligd protocol voor de uitwisseling van berichten;

— XML-berichten;

— op XML gebaseerde digitale ondertekening en versleuteling;

— VPN.

3.1.1. *Uitwisseling van berichten*

De communicatie tussen het register van de Unie en het Zwitserse register wordt gebaseerd op een mechanisme voor de uitwisseling van berichten via beveiligde kanalen. Elke partij bewaart de ontvangen berichten in een eigen register.

Beide partijen houden een logboek van de ontvangen berichten bij, alsmede van de gegevens betreffende de verwerking.

Fouten of een onverwachte status moeten als waarschuwing worden gemeld, en menselijk contact tussen de ondersteunende teams moet plaatsvinden.

Fouten en onverwachte gebeurtenissen worden behandeld met inachtneming van de in het kader van het incidentenbeheerproces van de GOP vastgestelde operationele procedures.

3.1.2. *XML-bericht — Beschrijving op hoog niveau*

Een XML-bericht bevat een van de volgende elementen:

— een of meer transactieverzoeken en/of een of meer transactieresponsen;

— een actie/respons in verband met de afstemming;

— een testbericht.

Elk bericht bevat een header met:

— het ETS-systeem waarvan het afkomstig is;

— een volgnummer.

3.1.3. *Opnamevensters*

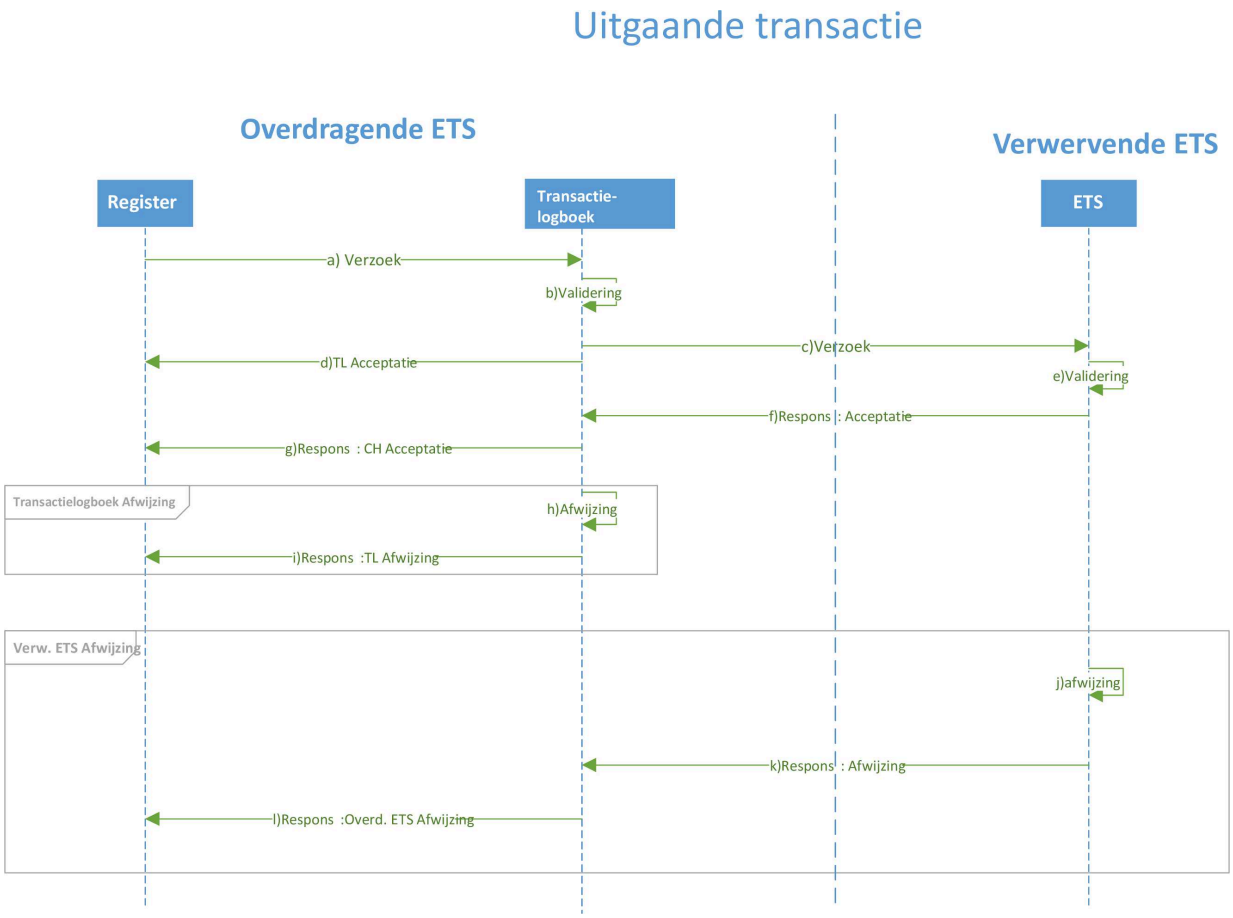
De permanente registerkoppeling is gebaseerd op vooraf gedefinieerde opnamevensters die worden gevolgd door een reeks van benoemde gebeurtenissen (“named events”). De via de verbinding ontvangen transactieverzoeken worden uitsluitend tijdens van tevoren vastgestelde tussenpozen opgenomen. Opnamevensters omvatten een technische validatie voor uitgaande en inkomende transacties. Daarnaast kunnen afstemmingen dagelijks worden uitgevoerd en manueel worden geactiveerd.

Wijzigingen in de frequentie en/of timing van een of meer van deze gebeurtenissen worden behandeld met inachtneming van de in het kader van de afhandeling van verzoeken van de GOP vastgestelde operationele procedures.

3.1.4. *Transactieberichtenstroom*

Uitgaande transactie

Dit is een weergave vanuit het perspectief van de ETS die de overdracht doet. De specifieke stroom wordt weergegeven in het volgende schema:



Hoofdstroom bestaande uit de volgende stappen (zoals in het schema hierboven):

a) bij de ETS die de overdracht doet, wordt het transactieverzoek van het register naar het transactielogboek verzonden zodra de bedrijfsvertraging voorbij is (24 uur vertraging, indien van toepassing);

b) het transactielogboek valideert het transactieverzoek;

c) het verzoek om een transactie wordt naar de ETS van bestemming verzonden;

d) de acceptatierespons wordt naar het register van de ETS van oorsprong verzonden;

e) de ETS van bestemming valideert het transactieverzoek;

f) de ETS van bestemming stuurt de acceptatierespons terug nar het transactielogboek van de ETS van oorsprong;

g) het transactielogboek stuurt de acceptatierespons naar het register.

Alternatieve stroom “Afwijzing door transactielogboek” (zoals in het schema hierboven, beginnend bij a) in de hoofdstroom):

a) in de ETS van oorsprong wordt het transactieverzoek van het register naar het transactielogboek verzonden zodra de bedrijfsvertraging voorbij is (24 uur vertraging, indien van toepassing);

b) het transactielogboek valideert het verzoek niet;

c) het afwijzingsbericht wordt verzonden naar het register van oorsprong.

Alternatieve stroom “Afwijzing door ETS” (zoals in het schema, beginnend bij d) in de hoofdstroom):

a) in de ETS van oorsprong wordt het transactieverzoek van het register naar het transactielogboek verzonden zodra de bedrijfsvertraging voorbij is (24 uur vertraging, indien van toepassing);

b) het transactielogboek valideert de transactie;

c) het verzoek om een transactie wordt naar de ETS van bestemming verzonden;

d) de acceptatierespons wordt naar het register van de ETS van oorsprong verzonden;

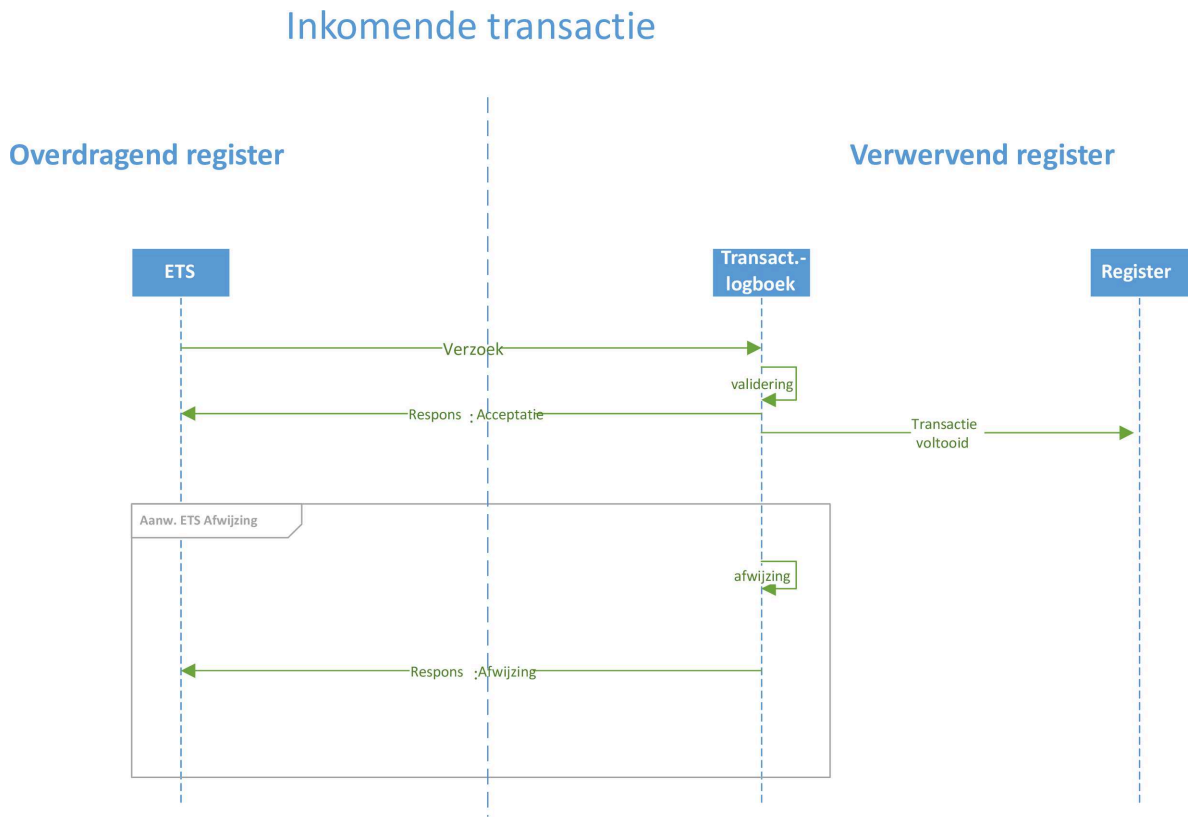
e) de het transactielogboek van de verwervende ETS valideert de transactie niet;

f) de verwervende ETS stuurt de afwijzingsrespons naar het transactielogboek van de overdragende ETS;

g) het transactielogboek stuurt de afwijzing naar het register.

Inkomende transacties

Dit is een weergave vanuit het perspectief van de verwervende ETS. De specifieke stroom wordt weergegeven in het volgende schema:



Het schema toont:

1) wanneer het transactielogboek van de verwervende ETS het verzoek valideert, stuurt het de acceptatierespons naar de overdragende ETS en een bericht “transactie voltooid” naar het register van de verwervende ETS;

2) wanneer een inkomend verzoek binnenkomt op het verwervende transactielogboek en wordt geweigerd, wordt het transactieverzoek niet naar het register van de verwervende ETS gestuurd.

Protocol

De transactieberichtencyclus omvat slechts twee berichten:

— overdragende ETS → verwervende ETS: transactievoorstel;

— verwervende ETS → overdragende ETS: transactierespons: acceptatie of afwijzing (met vermelding van de reden voor afwijzing):

  — acceptatie: de transactie is voltooid;

  — afwijzing: de transactie is beëindigd.

Transactiestatus

— De transactiestatus van de overdragende ETS wordt veranderd in "voorgesteld" wanneer het verzoek wordt verzonden.

— De transactiestatus van de verwervende ETS wordt veranderd in "voorgesteld" wanneer het verzoek wordt ontvangen en wordt behandeld.

— De transactiestatus van de verwervende ETS wordt veranderd in "voltooid"/"beëindigd" nadat het voorstel is verwerkt. De verwervende ETS stuurt vervolgens het bijbehorende bericht van acceptatie/afwijzing.

— De transactiestatus van de overdragende ETS wordt veranderd in "voltooid/beëindigd" nadat het bericht van acceptatie/afwijzing wordt ontvangen en verwerkt.

— In de overdragende ETS blijft de transactiestatus "voorgesteld" indien geen respons wordt ontvangen.

— De transactiestatus van de verwervende ETS geeft elke voorgestelde transactie die langer dan 30 minuten op "voorgesteld" staat, de status "beëindigd".

Incidenten in verband met transacties worden behandeld met inachtneming van de in het kader van het incidentenbeheerproces van de GOP vastgestelde operationele procedures.

3.2. **Beveiliging van gegevensoverdracht**

Verstuurde gegevens worden onderworpen aan vier beveiligingsniveaus:

1) controle van de toegang tot het netwerk: firewall en netwerkinterconnectie;

2) versleuteling tijdens het vervoer: VPN;

3) versleuteling tijdens sessie: overdrachtprotocol voor beveiligde uitwisseling van berichten;

4) versleuteling op niveau van de toepassing: XML-inhoudversleuteling en -ondertekening.

3.2.1. *Firewall en netwerkinterconnectie*

De koppeling wordt tot stand gebracht over een netwerk dat wordt beschermd door een op hardware gebaseerde firewall. De firewall moet zodanig worden geconfigureerd dat alleen "geregistreerde" clients verbindingen met de VPN-server kunnen maken.

3.2.2. *Virtueel particulier netwerk (VPN)*

Alle communicatie tussen de partijen wordt beschermd door middel van VPN-technologie (virtueel particulier netwerk). VPN-technologieën bieden de mogelijkheid om via een netwerk zoals het internet van de ene plaats naar de andere te "tunnelen", waarbij alle communicatie wordt beschermd. Voorafgaand aan het opzetten van de VPN-tunnel wordt een digitaal certificaat afgegeven aan het eindpunt van een mogelijke client, zodat de client bij het verbinden een bewijs van identiteit kan overleggen. Elke partij is verantwoordelijk voor de installatie van het certificaat in het eigen VPN-eindpunt. Door gebruik te maken van digitale certificaten krijgt elke VPN-server toegang tot een centrale autoriteit voor het uitwisselen van authenticatiegegevens. Bij het opzetten van de tunnel wordt versleuteling uitgevoerd, zodat alle communicatie via de tunnel wordt beschermd.

De VPN-eindpunten van de clients zijn zodanig geconfigureerd dat de VPN-tunnel permanent in stand wordt gehouden, zodat te allen tijde betrouwbare communicatie in realtime en in beide richtingen tussen de partijen mogelijk is.

In het algemeen gebruikt de Europese Unie de beveiligde trans-Europese diensten voor telematica tussen overheidsdiensten (S-TESTA) als een particulier IP-netwerk. Daarom is dit netwerk ook geschikt voor de permanente registerkoppeling.

3.2.3. *Uitvoering van IPSec*

Het gebruik van het IPSec-protocol om de site-to-site VPN-infrastructuur te vormen, zal zorgen voor site-to-site authenticatie, de integriteit van de gegevens en gegevensversleuteling. IPSec-VPN-configuraties zorgen voor de juiste authenticatie tussen twee eindpunten in een VPN-verbinding. De partijen identificeren en authenticeren de client op afstand via de IPSec-verbinding door middel van een digitaal certificaat dat wordt verstrekt door een door het andere einde erkende certificeringsautoriteit.

IPSec waarborgt ook de integriteit van alle communicatie via de VPN-tunnel. Gegevenspakketten worden gehashed en ondertekend door middel van de authenticatie-informatie die door het VPN is ingevoerd. De vertrouwelijkheid van de gegevens wordt ook gewaarborgd door IPSec-versleuteling mogelijk te maken.

3.2.4. *Overdrachtprotocol voor beveiligde uitwisseling van berichten*

De permanente registerkoppeling berust op meerdere versleutelingslagen voor de beveiligde uitwisseling van gegevens tussen de partijen. Beide systemen en hun verschillende omgevingen zijn op het niveau van het netwerk met elkaar verbonden door middel van VPN-tunnels. Op het niveau van de applicatie worden de bestanden overgedragen met behulp van een overdrachtprotocol voor de beveiligde uitwisseling van berichten op het niveau van de sessie.

3.2.5. *XML-versleuteling en -ondertekening*

In XML-bestanden vindt ondertekening en versleuteling plaats op twee niveaus. Elk(e) transactieverzoek, transactierespons en afstemmingsbericht wordt afzonderlijk digitaal ondertekend.

In een tweede stap wordt elk subelement van het “bericht”-element afzonderlijk versleuteld.

Als een derde stap en om de integriteit en onweerlegbaarheid van het volledige bericht te waarborgen, wordt bovendien het kernelementbericht digitaal ondertekend. Dit resulteert in een hoog niveau van bescherming voor de in XML ingebedde gegevens. Bij de technische uitvoering worden de normen van het World Wide Web Consortium in acht genomen.

Voor het ontsleutelen en verifiëren van het bericht wordt het proces in omgekeerde volgorde uitgevoerd.

3.2.6. *Cryptografische sleutels*

Voor versleuteling en ondertekening wordt gebruikgemaakt van een openbare cryptografische sleutel.

Voor IPSec worden alleen digitale certificaten gebruikt die zijn afgegeven door een door beide partijen vertrouwde certificeringsautoriteit (CA). Die CA is verantwoordelijk voor identiteitscontrole van de certificaathouder en de afgifte van certificaten die worden gebruikt om een organisatie te identificeren en beveiligde kanalen datacommunicatie tussen de partijen te op te zetten.

Cryptografische sleutels worden gebruikt voor het ondertekenen en versleutelen van communicatiekanalen en gegevensbestanden. De openbare certificaten worden door de partijen digitaal uitgewisseld door middel van beveiligde kanalen en geverifieerd buiten de band. Deze procedure maakt integraal deel uit van het proces informatiebeveiligingsbeheer van de GOP.

3.3. **Lijst van functies in het kader van de koppeling**

De koppeling specificeert het transmissiesysteem voor een reeks functies die de uit de overeenkomst voortvloeiende bedrijfsprocessen uitvoeren. De koppeling bevat eveneens de specificatie voor het afstemmingsproces en voor de testberichten die de uitvoering van heartbeatmonitoring mogelijk maken.

3.3.1. *Zakelijke transacties*

Vanuit het bedrijfsperspectief behandelt de koppeling vier (4) soorten transactieverzoeken:

— externe overdracht:

  — na de inwerkingtreding van de ETS-koppeling zijn EU- en CH-emissierechten fungibel, en dus volledig overdraagbaar tussen de partijen;

  — bij een overdracht via de koppeling zijn een overdragende rekening op de ene ETS en een verwervende rekening op de andere ETS betrokken;

  — de overdracht kan een of meer van de vier (4) soorten emissierechten omvatten:

    — Zwitserse algemene emissierechten (CHU);

    — Zwitserse luchtvaartemissierechten (CHUA);

    — algemene EU-emissierechten (EUA);

    — EU-luchtvaartemissierechten (EUAA);

— internationale toewijzing:

vliegtuigexploitanten die door de ene ETS worden geadministreerd met verplichtingen onder de andere ETS en recht hebben op kosteloze emissierechten van die tweede ETS, ontvangen kosteloze luchtvaartemissierechten van de tweede ETS via de internationale toewijzingstransactie;

— terugdraaiing van de internationale toewijzing:

deze transactie vindt plaats in het geval dat de kosteloze toewijzing van emissierechten aan een vliegtuigexploitant door de andere ETS geheel moet worden teruggedraaid;

— teruggave van overtollige toewijzing:

vergelijkbaar met terugdraaiing, maar de toewijzing hoeft niet geheel te worden teruggedraaid, en alleen de teveel toegewezen emissierechten moeten worden teruggegeven aan de toewijzende ETS.

3.3.2. *Afstemmingsprotocol*

Afstemmingen vinden pas plaats nadat de vensters voor de opname, validering en verwerking van berichten gesloten zijn.

Afstemmingen maken integraal deel uit van de beveiligings- en consistentiemaatregelen van de koppeling. De partijen moeten het exacte tijdstip van de afstemming overeenkomen alvorens een tijdschema op te stellen. Een dagelijks geplande afstemming kan plaatsvinden indien beide partijen daarmee instemmen. Na elke opname van berichten wordt ten minste één geplande afstemming uitgevoerd.

De partijen kunnen in elk geval te allen tijde handmatige afstemmingen initiëren.

Wijzigingen in de frequentie en timing van de geplande afstemming worden behandeld met inachtneming van de in het kader van de afhandeling van verzoeken van de GOP vastgestelde operationele procedures.

3.3.3. *Testbericht*

Voor het testen van het communicatietraject wordt in een testbericht voorzien. Het bericht bevat gegevens waarmee het bericht als test wordt herkend, en wordt na ontvangst door de andere partij beantwoord.

3.4. **Vereisten voor gegevensregistratie**

Om te beantwoorden aan de behoefte van beide partijen aan het bijhouden van accurate en consistente informatie en te voorzien in instrumenten voor het gebruik in het afstemmingsproces om inconsistenties weg te nemen, worden door beide partijen vier (4) soorten gegevensregisters bijgehouden:

— transactielogboeken,

— afstemmingslogboeken,

— berichtarchieven,

— logboeken van interne controle.

Alle gegevens in die logbestanden worden ten minste gedurende drie (3) maanden bewaard ten behoeve van het oplossen van problemen, en de verdere bewaring ervan voor controledoeleinden hangt af van het voor elke partij toepasselijke recht. Logbestanden ouder dan drie (3) maanden kunnen worden gearchiveerd in een beveiligde locatie in een onafhankelijk IT-systeem, op voorwaarde dat zij binnen een redelijke termijn kunnen worden opgevraagd of geconsulteerd.

Transactielogboeken

De subsystemen van het EUTL en het SSTL zijn transactielogboeken.

De transactielogboeken bevatten een registratie van elke voorgestelde transactie die naar de andere ETS wordt verzonden. Elke registratie bevat alle gegevensvelden van de transactie en de daaropvolgende uitkomst ervan (de respons van de ontvangende ETS). In de transactielogboeken wordt eveneens een register bijgehouden voor inkomende transacties alsmede voor de naar de ETS van oorsprong gestuurde respons.

Afstemmingslogboeken

Het afstemmingslogboek bevat een registratie van elk afstemmingsbericht dat tussen de partijen wordt uitgewisseld, met inbegrip van de afstemmingsidentificatiecode, het tijdstempel en het resultaat van de afstemming: de afstemmingsstatus “Pass” of “Discrepancies”. In de permanente registerkoppeling maken afstemmingsberichten integraal deel uit van de uitgewisselde berichten en worden zij daarom opgeslagen zoals beschreven onder “Berichtarchieven”.

Beide partijen registreren elk verzoek en de respons daarop in het afstemmingslogboek. Hoewel de informatie in het afstemmingslogboek tijdens de afstemming niet rechtstreeks wordt gedeeld, kan de toegang tot deze informatie noodzakelijk zijn om inconsistenties weg te nemen.

Berichtarchieven

Beide partijen moeten een kopie van de uitgewisselde (zowel verzonden als ontvangen) gegevens (de XML-bestanden) archiveren, met een vermelding of de XML-berichten in het juiste formaat waren verstuurd of niet.

Het belangrijkste doel van het archief is om in het kader van controles te kunnen nagaan wat van naar en van de andere partij is verzonden en ontvangen. Daartoe moeten behalve de dossiers ook de desbetreffende certificaten worden gearchiveerd.

Die dossiers zullen ook aanvullende informatie opleveren voor het oplossen van problemen.

Logboeken van interne controle

Deze logboeken worden door elke partij afzonderlijk gedefinieerd en gebruikt.

3.5. **Operationele vereisten**

De uitwisseling van gegevens tussen beide systemen is in de permanente registerkoppeling niet volledig autonoom; dit betekent dat exploitanten en procedures moeten worden ingeschakeld om de koppeling operationeel te maken. Daartoe worden in dit proces verschillende rollen en instrumenten in detail beschreven.

4. BESCHIKBAARHEIDSBEPALINGEN

4.1. Ontwerp voor de beschikbaarheid van de communicatie

De architectuur voor permanente registerkoppeling is een ICT-infrastructuur en software die de communicatie tussen de ETS van Zwitserland en het EU-ETS mogelijk maakt. Het waarborgen van een hoog niveau van beschikbaarheid, integriteit en vertrouwelijkheid van die gegevensstroom is derhalve een essentieel aspect dat moet worden meegenomen bij het ontwerp van de permanente registerkoppeling. Aangezien de ICT-infrastructuur, de op maat gemaakte software en de processen een integrale rol in dit project spelen, moeten alle drie de elementen in aanmerking worden genomen om een bestendig systeem te ontwerpen.

Bestendigheid van de ICT-infrastructuur

In het hoofdstuk betreffende algemene bepalingen worden de bouwblokken van de architectuur beschreven. Wat de ICT-infrastructuur betreft, wordt in de permante registerkoppeling een veerkrachtig VPN-netwerk opgezet dat veilige communicatietunnels creëert waarin beveiligde berichtenuitwisseling kan plaatsvinden. Andere elementen worden geconfigureerd voor een hoge beschikbaarheidsgraad en/of maken gebruik van terugvalmechanismen.

Bestendigheid van op maat gemaakte software

De op maat gemaakte softwaremodules vergroten de bestendigheid door de communicatie met de andere partij gedurende een bepaalde periode te trachten te herstellen indien die om welke reden dan ook niet beschikbaar is.

Bestendigheid van de dienst

De gegevensuitwisseling tussen de partijen gebeurt in de permanente registerkoppeling met vooraf bepaalde tussenpozen. Sommige van de stappen die vereist zijn in vooraf geplande gegevensuitwisseling vereisen handmatige tussenkomst van systeembeheerders en/of registeradministrateurs. Rekening houdend met dit aspect en met het oog op het vergroten van de beschikbaarheid en het succes van de uitwisselingen, worden de volgende maatregelen getroffen:

— de operationele procedures voorzien in tijdvensters voor de uitvoering van elke stap;

— de softwaremodules voor de permanente registerkoppeling passen asynchrone communicatie toe;

— in het kader van het automatische afstemmingsproces zal worden vastgesteld of er problemen zijn geweest bij de opname van gegevensbestanden aan beide zijden;

— de monitoringprocessen (ICT-infrastructuren en op maat gemaakte softwaremodules) worden in overweging genomen bij incidentbeheerprocedures en activeren deze (zoals gedefinieerd in de gemeenschappelijke operationele procedures). Die procedures, die gericht zijn op het verkorten van de tijd die nodig is om de normale werking te herstellen na incidenten, zijn essentieel om een hoge beschikbaarheidsgraad te waarborgen.

4.2. Initialisatie, communicatie, heractivering en testplan

Alle verschillende elementen van de architectuur van de permanente registerkoppeling moeten een reeks individuele en collectieve tests doorstaan om te bevestigen dat het platform klaar is wat de ICT-infrastructuur en het informatiesysteem betreft. Die operationele tests zijn een verplichte voorwaarde telkens wanneer het platform de permanente registerkoppeling doet overgaan van de status “buiten werking” naar de operationele status.

De activering van de operationele status van de koppeling vereist vervolgens de succesvolle uitvoering van een vooraf bepaald testplan. Dit bevestigt dat elk register eerst een reeks interne tests heeft uitgevoerd, gevolgd door een validering van de eind-tot-eindconnectiviteit voordat een begin wordt gemaakt met de indiening van productietransacties tussen beide partijen.

In het testplan moeten de algemene teststrategie en details over de testinfrastructuur worden vermeld. Voor elk element in elk testblok moet het testplan met name het volgende omvatten:

— de testcriteria en -instrumenten;

— de rollen die betrokken moeten zijn bij de uitvoering van de test;

— de verwachte resultaten (positief en negatief);

— het testschema;

— de voorschriften voor het registreren van de testresultaten;

— documentatie over het oplossen van problemen;

— bepalingen inzake escalatie.

Als proces kunnen de activeringstests voor de operationele status worden opgesplitst in vier (4) conceptuele blokken of fasen:

4.2.1. *Interne tests van de ICT-infrastructuur*

Die tests moeten door registeradministrateurs aan elk einde afzonderlijk worden uitgevoerd en/of gecontroleerd.

Elk onderdeel van de ICT-infrastructuur aan elk einde wordt afzonderlijk getest. Dit omvat elk afzonderlijk onderdeel van de infrastructuur. Die tests kunnen automatisch of manueel worden uitgevoerd, maar controleren of elk element van de infrastructuur operationeel is.

4.2.2. *Communicatietests*

Die tests worden afzonderlijk door elke partij geactiveerd en het beëindigen van de tests vergt de samenwerking van het andere einde.

Zodra individuele elementen operationeel zijn, moeten de communicatiekanalen tussen de beide registers worden getest. Daartoe controleert elke partij of de toegang tot het internet werkt, de VPN-tunnels zijn opgezet, en de IP-verbinding tussen de partijen werkt. De bereikbaarheid van de lokale infrastructuurelementen en die op afstand en de IP-connectiviteit moeten bij het andere einde worden bevestigd.

4.2.3. *Volledige systeemtest (eind-tot-eind)*

Die tests moeten aan beide einden worden uitgevoerd en de resultaten moeten met de andere partij worden gedeeld.

Zodra de communicatiekanalen en elk afzonderlijk onderdeel van beide registers zijn getest, moet elk einde een reeks gesimuleerde transacties en afstemming daarvan voorbereiden die representatief zijn voor alle functies die binnen de koppeling moeten worden uitgevoerd.

4.2.4. *Beveiligingstests*

Die tests moeten worden uitgevoerd en/of worden geactiveerd door registeradministrateurs aan elk einde en zoals beschreven in de hoofdstukken 5.4 “Richtsnoeren voor het testen van de beveiliging” en 5.5 “Bepalingen inzake risicobeoordeling”.

Pas nadat elk van de vier fasen/blokken met voorspelbare resultaten zijn voltooid, kan aan de permanente registerkoppeling de operationele status worden toegekend.

Testmiddelen

Elke partij hanteert specifieke testmiddelen (specifieke ICT-infrastructuursoftware en -hardware) en ontwikkelt testfuncties in hun respectieve systemen ter ondersteuning van de handmatige en doorlopende validatie van het platform. Handmatige individuele of coöperatieve testprocedures kunnen te allen tijde door registeradministrateurs worden uitgevoerd. Activering van de operationele status is van nature een handmatig proces.

Het is eveneens bepaald dat het platform op gezette tijden automatische controles uitvoert. Die controles zijn erop gericht de beschikbaarheid van het platform te vergroten door potentiële problemen met de infrastructuur of software in een vroeg stadium op te sporen. Dat platformmonitoringplan bestaat uit twee elementen:

— toezicht op ICT-infrastructuren: aan beide einden wordt de infrastructuur gemonitord door de aanbieders van de ICT-diensten. De automatische tests hebben betrekking op de verschillende infrastructuurelementen en de beschikbaarheid van communicatiekanalen;

— monitoring van de toepassing: monitoring van de toepassing: bij de softwaremodules van de permanente registerkoppeling wordt het communicatiesysteem gemonitord op het niveau van de applicatie (manueel en/of met regelmatige tussenpozen), waarbij de eind-tot-eind-beschikbaarheid van de koppeling wordt getest door een deel van de transacties over de verbinding te simuleren.

4.3. **Acceptatie-/testomgevingen**

De architectuur van het register van de Unie en het Zwitserse register bestaat uit de volgende drie omgevingen:

— productie (PROD): die omgeving bevat de daadwerkelijke gegevens en verwerkt daadwerkelijke transacties;

— acceptatie (ACC): die omgeving bevat niet-echte of geanonimiseerde, representatieve gegevens. Het is de omgeving waar systeembeheerders van beide partijen nieuwe releases valideren;

— test (TEST): die omgeving bevat niet-echte of geanonimiseerde, representatieve gegevens. Die omgeving is beperkt tot registeradministrateurs en is bedoeld voor het uitvoeren van integratietests door beide partijen.

Met uitzondering van het VPN zijn de drie omgevingen volledig onafhankelijk van elkaar, dat wil zeggen dat hardware, software, databanken, virtuele omgevingen, IP-adressen en poorten onafhankelijk van elkaar worden opgezet en functioneren.

Wat de indeling van het VPN betreft, moet de communicatie tussen de drie omgevingen volledig onafhankelijk zijn, hetgeen wordt gewaarborgd door gebruik te maken van S-TESTA.

5. **BEPALINGEN INZAKE VERTROUWELIJKHEID EN INTEGRITEIT**

Beveiligingsmechanismen en -procedures voorzien in een twee-personen-methode (4-ogen-principe) voor verrichtingen in de koppeling tussen het register van de Unie en het Zwitserse register. De twee-personen-methode is van toepassing wanneer dat nodig is. Zij is evenwel niet per definitie van toepassing op alle door de registeradministrateurs ondernomen stappen.

De beveiligingseisen worden in overweging genomen en behandeld in het beveiligingsbeheerplan, dat ook processen omvat die verband houden met de behandeling van beveiligingsincidenten als gevolg van een eventuele inbreuk op de beveiliging. Het operationele deel van die processen wordt beschreven in de GOP.

5.1. **Infrastructuur voor beveiligingstests**

Elke partij verbindt zich ertoe een beveiligingstestinfrastructuur op te zetten (door gebruik te maken van de gemeenschappelijke reeks van software en hardware die wordt gebruikt bij de opsporing van kwetsbaarheden in de ontwikkelings- en operatiefase):

— die is gescheiden van de productieomgeving;

— waar de beveiliging wordt geanalyseerd door een team dat onafhankelijk is van de ontwikkeling en de werking van het systeem.

Elke partij verbindt zich ertoe zowel statische als dynamische analyses uit te voeren.

In het geval van een dynamische analyse (zoals penetratietests) verbinden beide partijen zich ertoe de beoordelingen te beperken tot de test- en acceptatieomgevingen (zoals gedefinieerd in hoofdstuk 4.3 “Acceptatie-/testomgevingen”). Uitzonderingen op dit beleid moeten door beide partijen worden goedgekeurd.

Alvorens in de productieomgeving te worden uitgerold, moet de beveiliging van elke softwaremodule van de koppeling (zoals gedefinieerd in hoofdstuk 3.1 “Architectuur van de communicatieverbinding”) worden getest.

De testinfrastructuur moet zowel op het niveau van het netwerk als op het niveau van de infrastructuur worden gescheiden van de productie-infrastructuur. De beveiligingstests die nodig zijn om de naleving van de beveiligingsvereisten te controleren, worden in de testinfrastructuur uitgevoerd.

5.2. **Onderbreking van de koppeling en bepalingen betreffende heractivering**

Indien het vermoeden bestaat dat de veiligheid van het Zwitserse register, het SSTL, het register van de Unie of het EUTL in het gedrang is gekomen, stelt elke partij de andere daarvan onmiddellijk in kennis en onderbreekt ze de koppeling tussen het SSTL en het EUTL onmiddellijk;

De procedures voor het delen van informatie, voor een besluit tot onderbreking en voor een besluit tot heractivering maken deel uit van het proces inzake de inwilliging van verzoeken van de GOP.

Onderbreking

Onderbreking van de registerkoppeling overeenkomstig bijlage II bij de overeenkomst kan plaatsvinden om:

— administratieve redenen (bijvoorbeeld onderhoud), die gepland zijn;

— veiligheidsoverwegingen (of storingen in de IT-infrastructuur), die niet gepland zijn.

In noodgevallen stelt de ene partij de andere in kennis en onderbreekt zij de registerkoppeling unilateraal.

Indien wordt besloten de registerkoppeling te onderbreken, zorgt elke partij ervoor dat de koppeling op netwerkniveau wordt onderbroken (door onderdelen of alle inkomende en uitgaande verbindingen te blokkeren).

Het besluit tot al dan niet geplande onderbreking van de registerkoppeling wordt genomen volgens de procedure voor wijzigingsbeheer of beveiligingsincidentbeheer van de GOP.

Heractivering van de communicatie

Een besluit tot heractivering van de registerkoppeling zal worden genomen zoals uiteengezet in de GOP en in geen geval voordat de procedures voor het testen van de beveiliging met succes zijn afgerond, zoals beschreven in de hoofdstukken 5.4 “Richtsnoeren voor veiligheidstests” en 4.2 “Initialisering, heractivering van de communicatie en testplan”.

5.3. **Bepalingen inzake beveiligingsinbreuk**

Een beveiligingsinbreuk wordt beschouwd als een beveiligingsincident met gevolgen voor de vertrouwelijkheid en integriteit van alle gevoelige informatie en/of de beschikbaarheid van het systeem dat die informatie verwerkt.

Gevoelige informatie wordt in de lijst van gevoelige informatie vermeld en kan in het systeem of in enig gerelateerd onderdeel van het systeem worden verwerkt.

Informatie die rechtstreeks verband houdt met de beveiligingsinbreuk wordt als gevoelig beschouwd, met de vermelding “SPECIAL HANDLING: *ETS Critical*” aangemerkt en behandeld overeenkomstig de desbetreffende instructies, tenzij anders is bepaald.

Elke beveiligingsinbreuk wordt behandeld volgens het hoofdstuk betreffende beveiligingsincidentbeheer van de GOP.

5.4. **Richtsnoeren voor het testen van de beveiliging**

5.4.1. *Programmatuur*

Beveiligingstests, in voorkomend geval met inbegrip van de penetratietests, worden ten minste op alle nieuwe belangrijke softwarereleases uitgevoerd volgens de in de LTS vastgestelde beveiligingseisen om de beveiliging van de verbinding en de daaraan verbonden risico’s te beoordelen.

Indien in de afgelopen twaalf maanden geen belangrijke release is uitgekomen, wordt een beveiligingstest verricht op het huidige systeem, rekening houdend met de ontwikkelingen in de cyberdreiging die zich in de voorgaande twaalf maanden hebben voorgedaan.

De beveiligingstest van de registerkoppeling wordt uitgevoerd in de acceptatieomgeving en, indien vereist, in de productie-omgeving en met de coördinatie en wederzijdse overeenstemming van beide partijen.

Bij het testen van webapplicaties worden internationale open normen, zoals die welke zijn ontwikkeld door het Open Web Application Security Project (OWASP), in acht genomen.

5.4.2. *Infrastructuur*

De infrastructuur ter ondersteuning van het productiesysteem wordt regelmatig (ten minste eens per maand) gecontroleerd op kwetsbaarheden, en vastgestelde kwetsbaarheden worden hersteld volgens hetzelfde beginsel dat in het vorige hoofdstuk is uiteengezet, met gebruikmaking van een actueel register van kwetsbaarheden.

5.5. **Bepalingen inzake risicobeoordeling**

Indien de penetratietest van toepassing is, moet deze worden opgenomen in de beveiligingstest.

Elke partij kan voor de uitvoering van de beveiligingstests een beroep doen op een gespecialiseerde externe onderneming, mits die onderneming:

— beschikt over de vaardigheden en ervaring op het gebied van dergelijke beveiligingstests;

— niet rechtstreeks is verbonden aan de ontwikkelaar en/of zijn contractant, noch betrokken bij de ontwikkeling van de software van de verbinding, noch onderaannemer van de ontwikkelaar;

— een geheimhoudingsovereenkomst heeft ondertekend om de resultaten vertrouwelijk te houden en deze te behandelen op het niveau "SPECIAL HANDLING: *ETS Critical*" overeenkomstig de instructies voor behandeling.